Listing of Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Claim 1 (currently amended): A method for performing a cryptographic operation in a device under control of a security application, in which at least a part of a cryptographic value (y) is produced in the device, by a calculation utilizing a processor comprising at least one multiplication operation between a first (f_1) and a second (f_2) factor wherein one of said first and second factors includes a part that is a secret key (s) associated with the device, wherein said first factor (f_1) comprises a determined number of bits L in a first binary representation, wherein said second factor (f_2) comprises, in a second binary representation, several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L-1 bits set to 0, the method comprising:

obtaining a plurality (n) of successive binary versions of the first factor by shifting said first factor in accordance with the positions of the bits set to 1 of the second factor; and

carrying out the at least one multiplication operation by assembling said n successive binary versions of the first factor to produce said at least a part of the cryptographic value.

Claim 2 (previously presented): The method as claimed in claim 1, in which the secret key (s) forms part of an asymmetric cryptographic key pair associated with the device .

Claim 3 (previously presented): The method as claimed in claim 1, in which the device comprises a chip including hard-wired logic for producing the cryptographic value.

Claim 4 (previously presented): The method as claimed in claim 1, in which the calculation of the cryptographic value furthermore comprises an addition or a subtraction between a pseudo-random number (r) and the result of the multiplication.

Claim 5 (previously presented): The method as claimed in claim 4, in which the first and second factors (f_1, f_2) and the pseudo-random number (r) are dimensioned so that the pseudo-random number is greater than the result of the multiplication.

Claim 6 (original): The method as claimed in claim 5, in which the number of bits set to 1 of the second factor is chosen at most equal to the largest integer less than or equal to s_1/L, where s_1 is a predefined threshold less than the number of bits of the pseudo-random number (r) in binary representation.

Claim 7 (previously presented): The method as claimed in claim 1, in which the two factors of the multiplication include, as well as said part of the secret key (s), a number (c) provided to the device by the security application executed outside the device.

Claim 8 (previously presented): The method as claimed in claim 1, in which the two factors of the multiplication include, as well as said secret key (s), a number (c) provided by the device.

Claim 9 (previously presented): The method as claimed in claim 1, in which said part of the secret key (s) is said first factor (f_1) of the multiplication.

Claim 10 (previously presented): The method as claimed in claim 1, the method further comprising:

calculating intervals of like size in bits, said size corresponding to the total size of a usable space divided by the number of bits set to 1 of the second factor of the multiplication operation;

placing each shifted binary version in its respective interval as a function of a shift in accordance with the positions of the bits set to 1 of the second factor.

Claim 11 (previously presented): The method as claimed in claim 1, in which said part of the secret key (s) is the second factor (f_2) of the multiplication.

Claim 12 (original): The method as claimed in claim 11, in which the secret key (s) is stored in a memory support of the device by coding the positions of its bits set to 1.

Claim 13 (previously presented): The method as claimed in claim 11, in which the secret key (s) is stored in a memory support of the device by coding numbers of bits separating respectively lower bounds of intervals of (S-1)/(n-1) bits and lower bounds of blocks of bits allotted to the first factor (f_1) of the multiplication and each disposed in the associated intervals, S being the number of bits of the secret key (s) and n the number of bits set to 1 of the secret key (s).

Claim 14 (previously presented): The method as claimed in claim 11, in which the secret key (s) is stored in a memory support of the device by coding numbers of bits, each representative of the number of bits separating two blocks of successive bits allotted to the first factor (f_1) of the multiplication.

Claim 15 (previously presented): The method as claimed in claim 1, in which the cryptographic value (y) is produced so as to authenticate the device in a transaction with the security application executed outside the device.

Claim 16 (previously presented): The method as claimed in claim 1, in which the cryptographic value (y) is produced in the guise of electronic signature.

Claim 17 (currently amended): A device with cryptographic function, comprising:

means of interfacing with a security application; and

means of calculation for producing <u>at least a part of</u> a cryptographic value (y), the means of calculation comprising:

means of multiplication between a first (f_1) and second (f_2) factor wherein one of said first and second factors includes a part that is a secret key (s) associated with the device,

wherein the first factor (f_1) comprises a determined number of bits L in a first binary representation and the second factor (f_2) comprises, in a second binary representation, several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L – 1 bits set to 0, wherein [[the]] <u>said at least a part of a</u> cryptographic value (y) comprises a result of the multiplication between the first and second factors, wherein the means of

multiplication comprises means for assembling a plurality (n) of successive binary versions of the first factor, wherein said n successive binary versions are obtained by shifting said first factor in accordance with the positions of the bits set to 1 of the second factor.

Claim 18 (previously presented): The device as claimed in claim 17, furthermore comprising means of generating a pseudo-random number (r), the means of calculation comprising means for adding the result of the multiplication to or subtracting it from said pseudo-random number.

Claim 19 (previously presented): The device as claimed in claim 18, in which the first and second factors (f_1, f_2) and the pseudo-random number (r) are dimensioned so that the pseudo-random number is greater than the result of the multiplication.

Claim 20 (previously presented): The device as claimed in claim 17, in which the means of calculation are embodied as hard-wired logic.

Claim 21 (previously presented): The device as claimed in claim 17, in which said part of the secret key (s) is the first factor (f_1) of the multiplication.

Claim 22 (previously presented): The device as claimed in claim 17, in which said part of the secret key (s) is the second factor (f_2) of the multiplication.

Claim 23 (previously presented): The device as claimed in claim 22, furthermore comprising a memory adapted for storing data for coding the positions of the bits set to 1 of the secret key (s).